第37卷 第14期 计 算 机 工 程 2011年7月
Vol.37 No.14 Computer Engineering July 2011

·安全技术· 文章编号：1000—3428(2011)14—0128—03 文献标识码：A 中图分类号：TP309

多 Agent 系统中基于狄利克雷分布的信任模型

陈广福，蔡国永，林 航，王瑞丽，刘国宾

(桂林电子科技大学计算机科学与工程学院，广西 桂林 541004)

摘 要：提出一种多 Agent 系统中基于狄利克雷分布的信任模型。该模型利用狄利克雷分布解决二元评价的局限性，使信任模型可以按等级来评价信誉。提出层次过滤算法，以解决推荐信息中存在的各类恶意 Agent 问题。仿真实验结果表明，该信任模型能有效抑制不诚实推荐和策略性欺骗。

关键词：狄利克雷分布；多 Agent 系统；信任；过滤算法

Trust Model Based on Dirichlet Distribution in Multi-Agent System

CHEN Guang-fu, CAI Guo-yong, LIN Hang, WANG Rui-li, LIU Guo-bin

(School of Computer Science and Engineering, Guilin University of Electronic Technology, Guilin 541004, China)

【**Abstract**】This paper proposes a trust model based on Dirichlet distribution in Multi-Agent System(MAS). It uses the Dirichlet distribution to solve the limitations of a binary evaluation, the trust model can rate with graded levels. A level filtering algorithm is proposed to effectively filter a variety of malicious Agent in the referrals. Experimental results show that the proposed trust model is effective in inhibiting unfair recommendations and strategies deception.

【**Key words**】Dirichlet distribution; Multi-Agent System(MAS); trust; filtering algorithm

DOI: 10.3969/j.issn.1000-3428.2011.14.042

1 概述

多 Agent 系统(Multi-Agent System, MAS)正朝着大规模、开放、动态和分布式结构的方向发展。在 MAS 中，Agent 由追求不同利益的拥有者所占有，并且可以在任何时间加入或离开系统，具有自私性和不可靠性；同时没有 Agent 能确知环境的一切信息，也不存在一个中心控制 Agent 可以控制所有 Agent。这些特点使 Agent 信任研究，特别是信任评估模型的研究成为近年来 MAS 研究的热点。

许多学者从不同角度提出了各类信任评估模型。文献[1]提出了 Beta 信誉系统(Beta Reputation System, BRS)，该模型采用基于 Beta 分布函数描述二项事件(binary event)后验概率的思想，同时提供了一套主观逻辑算子，用于计算信任度。其不足之处是只能用于对信誉二元评价的情形。文献[2]扩展了 BRS 系统，提出了迭代的过滤恶意推荐算法，该模型同样只适用于二元评价情形，并且只有在提供者提供服务是真实和准确的情况下有效。文献[3]提出了基于 Agent 虚拟组织的信任与信誉模型(TRAVOS)，该模型采用概率论研究信息不精确条件下个体 Agent 之间的信任关系，其不足之处是使用了二元来表示交互结果评估，且在过滤不准确推荐机制中，没有考虑足够多的直接交互经验，不能对付策略性欺骗行为；文献[4]提出了 Dirichlet 信誉系统(Dirichlet Reputation System, DRS)，给出了一种基于 Dirichlet 分布的信任算法，该算法主要考虑如何利用 Dirichlet 概率分布分布理论计算信任度，没有过多考虑抵抗多种恶意攻击。其不足之处是没有考虑如何识别恶意评价以及对恶意评价惩罚且仅仅利用直接评价结果计算信任度，没有考虑推荐信任。文献[5]提出一种可信区间方法处理虚假推荐，但该方法的不足之处是当有大量不同级别恶意节点时，算法处理恶意节点能力就会降低，这是因为算法中也用到 Beta 分布。

在上述信任模型的基础上，本文提出一种基于狄利克雷分布的信任模型(Dirichlet-Based Distribution Trust Model, DBTM)。

2 基于狄利克雷分布的信任模型

关于信任，目前尚无一致认同的定义。一般认为，信任是一种主观信念，可理解成一个实体评价其他实体行为的主观可能性程度。在 MAS 中，接收服务称为信任者，用 Ag_{tr} 表示，提供服务称为被信任者，用 Ag_{te} 表示。根据评价依据获得方式的不同，信任评价可以分为 2 类：直接信任和推荐信任。用 θ 来表示 Ag_{tr} 和 Ag_{te} 间交互成功的概率。直接信任是通过 Ag_{tr} 和 Ag_{te} 间的直接交互经验获得的信任评价，用 θ_{dir} 表示。推荐信任是通过推荐 Agent 提供的反馈信息获得的信任评价，用 θ_{rec} 表示。

$\hat{\theta}_{\mathrm{dir}}$ 表示直接信任度，$\hat{\theta}_{\mathrm{rec}}$ 表示推荐信任度，$\hat{\theta}$ 来表示信任度，它是直接信任度和推荐信任度合并成，其计算式如下：

$$\hat{\theta}=\omega_1\hat{\theta}_{\mathrm{dir}}+\omega_2\hat{\theta}_{\mathrm{rec}} \tag{1}$$

其中，ω_1 和 ω_2 是决定 2 种概率重要性权重，且满足 $\omega_1+\omega_2=1$。其值由 Agent 的主观因素决定。

2.1 狄利克雷分布

狄利克雷分布是多项分布，可以对离散集进行评价。假

基金项目：广西自然科学基金资助项目(0728089)；广西研究生教育创新计划基金资助项目(2009105950812M18)

作者简介：陈广福(1979－)，男，硕士研究生，主研方向：多 Agent 系统，信任模型，机器学习；蔡国永，教授、博士；林 航、王瑞丽、刘国宾，硕士研究生

收稿日期：2011-01-14 **E-mail：**cgf21st@163.com

设离散随机变量 X 有 x_1,x_2,L,x_k 共 k 个可能状态，对 X 多重采样服从狄利克雷分布。用 X 表示对 k 个离散随机元素的评价结果。则 X_i 表示第 i 个评价值，如：Good 或 Average，其集合为 $D=\{X_1=x_1,X_2=x_2,\mathrm{L},X_k=x_k\}$。设离散随机向量 $\boldsymbol{\gamma}=\{\gamma_1,\gamma_2,\mathrm{L},\gamma_k\}$ 表示 x 的概率密度分布($1\leqslant i\leqslant k$，$\sum_{i=1}^{k}\gamma_i=1$)，例如：$\boldsymbol{\gamma}(X=x_i)=\gamma_i$。$p(\boldsymbol{\gamma}\mid\xi)$ 表示给定知识背景下 $\boldsymbol{\gamma}$ 的概率密度函数。设离散随机变量 $\boldsymbol{\alpha}=\{a_1,a_2,\mathrm{L},a_k\}$ 表示 x 的观察值，这里称 $\{a_1,a_2,\mathrm{L},a_k\}$ 为超级参数。$\boldsymbol{\gamma}$ 的先验概率密度为：

$$p(\boldsymbol{\gamma}\mid\xi)=Dir(\boldsymbol{\gamma}\mid a_1,a_2,\mathrm{L},a_k)=\frac{\Gamma(\sum_{i=1}^{k}a_i)}{\prod_{i=1}^{k}\Gamma(a_i)}\prod_{i=1}^{k}\gamma_i^{a_i-1} \tag{2}$$

其中，ξ 表示背景知识；a_1,a_2,L,a_k 都大于 0；记 $\boldsymbol{\gamma}\mid\xi\sim Dir(a_1,a_2,\mathrm{L},a_k)$，可以求出狄利克雷分布期望值为：

$$E(p(\boldsymbol{\gamma}\mid\xi))=\frac{a_i}{\sum_{i=1}^{k}a_i} \tag{3}$$

2.2　直接信任度

在 MAS 中，Ag_{tr} 和 Ag_{te} 间的直接信任是对 Agent 历史交互经验的总结，因此直接信任度可以使用贝叶斯估计方法对 θ_{dir} 估计。

假设 Ag_{tr} 和 Ag_{te} 间已发生了 N 次交互。要评价 k 个离散随机元素，在这里，用 N_1,N_2,L,N_k 记录集合 D 中 X_i=x_i 出现的次数，其集合为 $N=\{N_1,N_2,\mathrm{L},N_k\}$，集合 N 是集合 D 的充分统计量。$\boldsymbol{\gamma}$ 的先验分布是狄利克雷分布，且狄利克雷分布是共轭分布，所以后验概率分布 $p(\boldsymbol{\gamma}\mid D,\xi)$ 也服从狄利克雷分布，推理如下：

$$p(\boldsymbol{\gamma}\mid D,\xi)\propto P(D\mid\boldsymbol{\gamma},\xi)P(\boldsymbol{\gamma}\mid\xi)\propto \prod_{i=1}^{k}\gamma_i^{N_i}\prod_{i=1}^{k}\gamma_i^{a_i-1}\propto\prod_{i=1}^{k}\gamma_i^{N_i+a_i-1} \tag{4}$$

后验分布与先验分布有相同的形式，因此，狄利克雷分布是共轭分布。则后验分布参数为：

$$\alpha_1+N_1,\alpha_2+N_2,\mathrm{L},\alpha_k+N_k$$

则有 $p(\boldsymbol{\gamma}\mid D,\xi)=Dir(\boldsymbol{\gamma}\mid a_1+N_1,a_2+N_2,\mathrm{L},a_k+N_k)$，$\boldsymbol{\gamma}$ 的后验分布期望估计值就是要求的直接信任度。

$$\hat{\gamma}=E(P(\boldsymbol{\gamma}\mid D,\xi)=\frac{\int_0^1\boldsymbol{\gamma}\prod_j^k\gamma_j^{a_j+N_j-1}\mathrm{d}\boldsymbol{\gamma}}{Dir(\boldsymbol{\gamma}\mid a_1+N_1,\mathrm{L},a_k+N_k)}=\frac{a_i+N_i}{\alpha+N} \tag{5}$$

$$\hat{\theta}_{\mathrm{dir}}=\hat{\gamma}=\frac{a_i+N_i}{\alpha+N} \tag{6}$$

2.3　推荐信任度

在 MAS 中，Ag_{tr} 和 Ag_{te} 在交互之前不认识或只有少量的交互的情况下要发生交互，就要考虑来自第三方的推荐信息。为使推荐信任度更加精确，用最优无偏估计方法对推荐信任度进行估计。假设 Ag_{tr} 和推荐 Agent，推荐 Agent 和 Ag_{te} 之间交互是相互独立的，它们的直接交互信任度分别为 $\hat{\theta}_1$、$\hat{\theta}_2$。交互次数分别为 U 和 V 次，这里设它们分别评价 m 个和 j 个离散随机元素，用 U_1,U_2,L,U_m 和 V_1,V_2,L,V_j 记录 D 中 X_i=x_i 出现次数，其集合分别为 $U=\{U_1,U_2,\mathrm{L},U_m\}$ 和 $V=\{V_1,V_2,\mathrm{L},V_j\}$，$U$、$V$ 也是 D_1 和 D_2 的充分统计量，D_1 和 D_2 是 D 的子集。由于狄利克雷分布是共轭分布，因此后验概率分布 $p(\boldsymbol{\gamma}\mid D_1,\xi)$ 和 $p(\boldsymbol{\gamma}\mid D_2,\xi)$ 也服从狄利克雷分布，后验分布分别为 $p(\boldsymbol{\gamma}\mid D_1,\xi)=Dir(\boldsymbol{\gamma}\mid a_1+U_1,a_2+U_2,\mathrm{L},a_m+U_m)$ 和 $p(\boldsymbol{\gamma}\mid D_2,\xi)=Dir(\boldsymbol{\gamma}\mid a_1+V_1,a_2+V_2,\mathrm{L},a_j+V_j)$，$p(\boldsymbol{\gamma}\mid D_1,\xi)$ 和 $p(\boldsymbol{\gamma}\mid D_2,\xi)$ 的数学期望估计值就是 $\hat{\theta}_1$、$\hat{\theta}_2$ 的信任度。根据狄利克雷分布的基本性质，2 个分布数学期望 $E(p(\boldsymbol{\gamma}\mid D_1,\xi))$、$E(p(\boldsymbol{\gamma}\mid D_2,\xi))$ 为 $\boldsymbol{\gamma}$ 的最优无偏估计量，即有：

$$\hat{\theta}_1=E(p(\boldsymbol{\gamma}\mid D_1,\xi))=\int\boldsymbol{\gamma}Dir(\boldsymbol{\gamma}\mid a_1+U_1,a_2+U_2,\mathrm{L},a_m+U_m)\mathrm{d}\boldsymbol{\gamma}=\frac{a_i+U_i}{\sum_{i=1}^{k}a_i+\sum_{i=1}^{k}U_i} \tag{7}$$

同理可以求出 $\hat{\theta}_2$：

$$\hat{\theta}_2=E(p(\boldsymbol{\gamma}\mid D_2,\xi))=\frac{a_i+V_i}{\sum_{i=1}^{k}a_i+\sum_{i=1}^{k}V_i} \tag{8}$$

采用概率链式法则来合成推荐信任度，即：

$$\hat{\theta}_{\mathrm{rec}}=\frac{a_i+U_i}{\sum_{i=1}^{k}a_i+\sum_{i=1}^{k}U_i}\cdot\frac{a_i+V_i}{\sum_{i=1}^{k}a_i+\sum_{i=1}^{k}V_i} \tag{9}$$

3　恶意 Agent 的过滤机制

由于 DBTM 也采用了将第三方推荐作为计算信任参考量之一，因此就存在第三方推荐所推荐的信息是否可靠的问题。推荐 Agent 为了获得最大利益或实现自己某一个目标，就会给出虚假推荐或是策略性欺骗。推荐 Agent 集合中有提供好的服务 Agent，也有提供一般服务 Agent，更甚至有提供虚假信息的恶意 Agent，混淆对 Agent 的信任评价。为了有效抑制不诚实推荐和策略性欺骗，提出了层次过滤算法。

假设存在一个推荐信任阈值，用 $\eta\in[0,\ 1]$来表示，当推荐信任度小于 η 时，认为推荐信任不诚实的；当推荐信任度大于 η 时，认为推荐信任是相对可信。因为有部分有良好推荐 Agent 策略性提供虚假信息，为了让算法更加有效，引入时间衰退因子，用 $\lambda\in[0,\ 1]$表示，交互了一段时间后，对各个层次上推荐信息累积和更新，用 ω_n 表示经过 n 次交互后，各层累积评价值。用 $\beta\in[0,1]$ 表示惩罚因子，h 表示对累积评价中恶意 Agent 处罚后集合。R 表示推荐信任集合，集合中任一个推荐者的信任度用 T 表示。层次过滤算法主要思想是，从推荐集中先过滤不诚实的推荐，然后从这些相对可信推荐中，找出偏离大多数的推荐信息。层次过滤算法如下：

```
1 Agtr 是信任者;
2 Agte 是被信任者;
3 R 是推荐集合;
4 ri 是 R 任一个推荐者;
5 T 是 R 任一推荐任信度;
6 if(T(γ)<η) then     // γ 等于推荐信任度，小于 η 认为是虚
//假推荐
7 从 R 中删除 ri ;
8  else
9  repeat
10  for( each ri in R) do
11  θ=ω1θdir+ω2θrec  //结合狄利克雷分布和直接经验进行整体
//评价
13  ωn = λ × θdir + θdir,n ; //对各个层次推荐 agent 进行累积评价
14  h=β.ωn ;  //对累积评价后的诋毁和协同作弊 Agent 进行
//处罚
15  if(T(γ)<η) then
16  从 R 中删除 ri ;
17  endif;
18  endfor;
19  endif;
20  until(直到 R 中推荐者不再变化);
21  return R;
```

4　仿真实验与分析

仿真基于 Agent 信誉和信任测试(Agent Repuation and

Trust, ART)平台，ART 的目标是建立统一的信誉系统测试平台。ART 有 2 种功能：作为实验平台，提供了配套的可视化工具及分析手段；作为竞赛平台，参与者可以编写 Agent 参与竞争。ART 作为实验平台使用时，可以取消竞赛中的部分限制，便于对采用不同策略的 Agent 在同一环境中，从不同的方面进行比较。

实验目的是评估所提出的信任模型在抑制不诚实推荐和策略性欺骗性能，并与模型 BRS、TRAVOS 相比较。假设电子市场为模拟场景，在该市场中，每个 Agent 承担 2 种角色：(1)服务提供者 Agent，它主要是提供服务。为简化复杂性，假设只有一种服务提供类型且所有的提供者 Agent 提供相同服务。(2)服务消费者 Agent，它与服务提供者进行交互且使用这些服务。

在服务提供者 Agent 中根据行为表现进行分类，如表 1 所示。

表 1 服务提供者 Agent 分类

服务提供者 Agent 类别	行为描述	符号
善意 Agent	提供好的服务且对其他 Agent 的评价都真实	S
简单恶意 Agent	只提供不真实的服务	SE
不诚实推荐 Agent	提供不真实服务，同时诋毁所有与之交互的 S 类 Agent，提交不诚实的评价信息	EL
策略恶意 Agent	只提供不真实服务，且与 S 类 Agent 时互采取策略性欺骗的行为，如行为摇摆	CE

仿真参数设置如下：在电子市场中，假设总的 Agent 数为 1 000 个，服务提供者 Agent 总数为 100，消费者 Agent 为 900 个，各类恶意 Agent 占的比例为[0.0~0.6]，模拟的次数为 20，仿真实验结果为平均值。每轮运行后有 10 个 Agent 离开同时也有 10 个 Agent 加入。时间衰减因子 λ=0.3，惩罚因子 β=0.5。仿真基于 Java 实现。

每次交互后，服务消费者是通过对每类服务提供者提供的服务质量进行评价，产生的评价越精确，会拥有越多的消费者，消费者选择每类服务得到相应的效益就高。本文用收支平衡(bank balance)表示消费者最后所得到的总效益。收支平衡值越大，表明成功交易率增加，提供者提供服务质量就好。因此，本文采用收支平衡来衡量 3 个不同信任模型抵抗恶意攻击能力。

4.1 SE 类仿真

简单恶意 Agent 的收支平衡对比如图 1 所示。

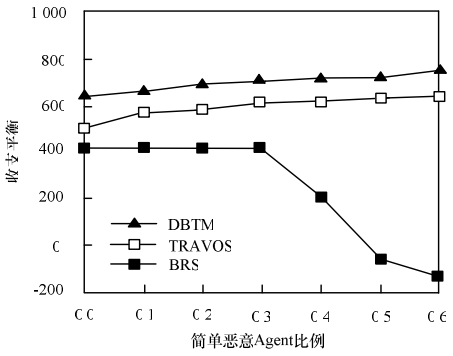

图 1 简单恶意 Agent 的收支平衡对比

可以看出，当恶意 Agent 提供不真实服务时，在恶意 Agent 占的比例比较少的情况下，DBTM 和 TRVAOS 都是有效识别恶意 Agent，而 BRS 的识别能力就比较差。随着恶意 Agent 增加到 30%，BRS 就直线下降，这是因为 BRS 系统中认为多数提供者提供的服务是真实和准确的。TRAVOS 到恶意 Agent 到达 60%时，收支平衡还是在上升，这是因为 TRAVOS 中依靠个人经验和第三方意见能有效处理简单恶意 Agent 发布不公平信息。DBTM 中收支平衡一直在增加，因为在 DBTM 中的过滤算法在开始阶段就能有效过滤掉这些简单恶意 Agent。

4.2 EL 类仿真

不诚实推荐 Agent 的收支平衡对比如图 2 所示。

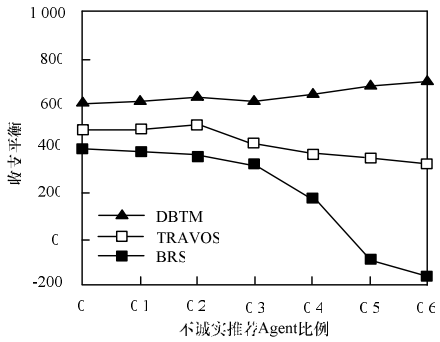

图 2 不诚实推荐 Agent 的收支平衡对比

可以看出，当恶意 Agent 占的比例较小时，三者的区别不是很大。当恶意 Agent 比例增大，DBTM 模型的性能显示出很大的优势。这是因为本文提出层次过滤算法能有效过滤不诚实推荐和诋毁 Agent 对 S 类 Agent 发布的不公正信息，使得 DBTM 有效识别诋毁 Agent。当比例到达 30%时有所下降，这是因为惩罚因子正在对诋毁 Agent 进行惩罚。而 BRS 系统直线下降，因为在 BRS 中没有惩罚机制，无法识别诋毁 Agent。同理，TRAVOS 模型恶意 Agent 到了 20%以后，由于不诚实推荐的信息和诋毁 Agent 发布不公正信息增多，模型中没有惩罚机制，单依靠个人经验和第三方意见不能识别，因此收支平衡也是在下降。

4.3 CE 类仿真

策略恶意 Agent 的收支平衡对比如图 3 所示。

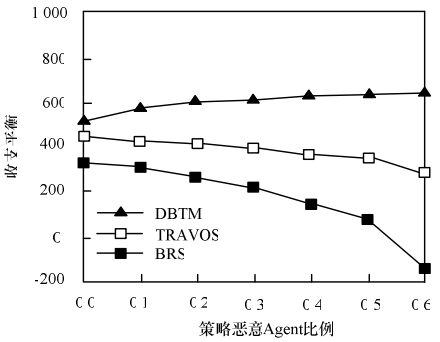

图 3 策略恶意 Agent 的收支平衡对比

可以看出，随着策略恶意 Agent 的增加，BRS 系统的收支平衡一直在下降，BRS 系统无法识别策略性恶意 Agent，导致成功交易率下降。类似的 TRAVOS 模型也是无法识别策略性欺骗 Agent，TRAVOS 模型没有考虑到行为的动态性。随着策略恶意 Agent 的比例增加，收支平衡也随着大幅下降。在 DBTM 模型中，过滤算法可以过滤大多策略恶意 Agent 给出的虚假评价和不公正信息，收支平衡也随之增加。

5 结束语

本文提出一种多 Agent 系统中基于狄利克雷分布的信任模型。该模型利用狄利克雷分布后验分布计算直接信任度，

(下转第 133 页)